Design and Implementation of a Software-Defined Data Authentication Algorithm for RFID Applications

VLSI Implementation for RFID Digest Code

Emad Waguih EL-SHEWEKH
R&D / Engineering Dept. Manager, Alfa Electronics.
Master Student,
Arab Academy for Science & Technology (AAST).
Cairo, Egypt.
ewaguih@emadwaguih.info

Khaled Ali SHEHATA
Chairman, Graduate Studies Dept., Engineering Collage,
Arab Academy for Science & Technology (AAST).
Cairo, Egypt.
k_shehata@aast.edu

Mohamed Ali ABOUL-DAHAB
Director of Quality Assurance Unit, Ministry of Education,
Arab Republic of Egypt.
Cairo, Egypt.
mdahab@aast.edu

Abstract – **In this paper we present a RFID data authentication using a digest code for the pre-paid cards which is one of the important issues to protect the money stored on these cards from attack, prevent card cloning and data interrogation.**
In this paper new authentication algorithm with self programmed architecture has been designed using Mentor Graphic FPGA Advantage, tested using Agilent Digital Logic Analyzer and implemented on a field programmable gate array (FPGA) Xilinx Spartan-3E XC3E500E-5FG320. Comparison took place between the simulation results from ModelSim program and the testing results from the Digital Logic Analyzer and a satisfying result has been obtained.
The authentication algorithm works with the same standards RFID transponders increasing their security and gives it the ability to work with standalone read/write RFID devices.
The cryptography procedure used with the RFID data authentication technique is the digest code for the transponder data to be saved on the transponder itself and to be checked in every operation for approving that the data on the transponder is genuine. The digest code is regenerated if the data changed and saved on the RFID card.
This authentication algorithm with the digest code generation does not need any backbone network or database or even computer. It is all done using the read/write RFID device.

Index Terms – RFID Authentication Algorithm; RFID Data Authentication; Encrypted data authentication Algorithm; VLSI Design for RFID Digest Code; FPGA Implementation; RFID Security System; RFID Data Protection; RFID Digest Code.

I. INTRODUCTION

Recently the contactless ID systems called Radio Frequency Identification (RFID) systems become very popular for contactless automatic identification. It will become the most common form of electronic data-carrying devices in use in everyday life within few years.

RFID cards are used in many applications like access control, pre-paid card, electronic wallet and others. Some of these applications need high security and data protection against cloning or data change especially for standalone systems. That is why we select this point to work on "Digest code for RFID Cards" for standalone systems and using a programmable algorithm to be programmed automatically through the card identification number.

The new authentication code algorithm does not need any calculations inside the card itself to keep the card cheep as possible. It depends on primitive polynomial that is selected from a pool of polynomials depending on the card ID. As well there is some random LUT to select polynomial shuffling among the selected polynomials and a bit shuffling too. All of these operations let the operation be a one way non-traceable operation.

The new authentication code called a "Digest Code". It prevents card cloning for RFID transponders and cards, as well as prevents card data change.

II. ARCHITECTURE

The RFID Digest code is the first authentication technique for RFID cards that work for standalone readers with no need for backbone servers and can do full data authentication against data modification or card cloning.

A. RFID Digest Code Properties

The proposed RFID Authentication technique must include the whole data packet with some information stored inside the reader and other related to the RFID card itself as the EPC Card ID with length of 64 or 96 bits [1], [2], [3].

TABLE I. AUTHENTICATION ALGORITHM DATA STRUCTURE.

EPC CARD ID (64 Bits) or (96 Bits)	**Data** (Variable Length)

B. Polynomial Characteristics

Our system works with a dozen of polynomials that are selected from a pool of different polynomials with different polynomials degree.

The smallest polynomial order is 8 bit; the largest polynomial order is 32 bit, in between there is 10, 11, 12, 15, 16, 24, and 30. These CRC Polynomials have been chosen for being primitive polynomials.

A degree (r) polynomial is primitive if and only if its period is 2^r-1. The period of a polynomial is the maximum period realized by its corresponding LFSR implementation.

Like prime numbers, primitive polynomials have the property that they cannot be factored into smaller degree polynomials in the defining field. Polynomials that cannot be factored into smaller degree polynomials are called irreducible. All primitive polynomials are irreducible.

However, not all irreducible polynomials are primitive. For example, $x^4+x^3+x^2+x+1$ is an irreducible polynomial but is not primitive. If 2^r-1 is a prime number then all degree-r irreducible polynomials are primitive [4].

C. Authentication code (Digest Code) Structure

The proposed authentication code (Digest Code) structure is composed of twelve polynomials output. Each polynomial output consists of 32 bit packet length. So the authentication code length is 12x32bit equal 384 bit length. This code can be used as it is, we can decrease the twelve polynomial to any number depend on the application and the data packet length we will work on. As well we can truncate the number of bits for every signal polynomial and use it with the card as a digest code. So we have a digest code starts from 8 bits up to 384 bits.

III. DESIGN PARAMETERS

A. Programmed Algorithm

It is a reconfigurable Algorithm that has the ability to restructure the already implemented algorithm using an input signal or code to have a different algorithm using the same resources of the hardware chip.

B. Multipurpose RFID Card

Multipurpose RFID card is to use the same card with Multi-Applications. Every application has its own memory locations and has its own security and authentication code independently on each other.

IV. SYSTEM IMPLEMENTATION

A. Authentication Code (Digest Code) Algorithm

The following flow chart in Figure 1 describes the design of the authentication code (Digest Code) creation and verification.

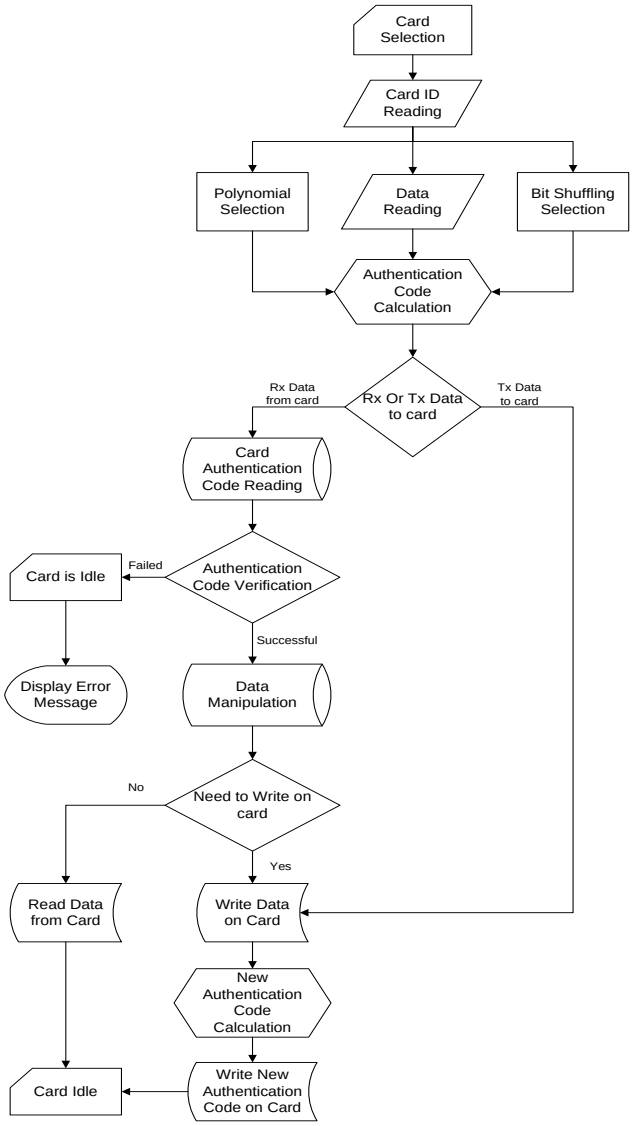

Figure 1. Flow Chart of the Authentication Code Algorithm

After card selection the RFID reader reads the card ID then a polynomial selection is done depending on the card ID that selects a new algorithm and new criteria in bit shuffling that will be used during digest code generation for the data read from the RFID card.

After calculating the authentication code for the data on the card a comparison takes place between the generated code and the saved code for authentication.

Successful authentication code verification leads to successful access to the system for data manipulation. New authentication code (Digest Code) will be generated to be saved with the new data on the RFID card.

B. *Design Hierarchy*

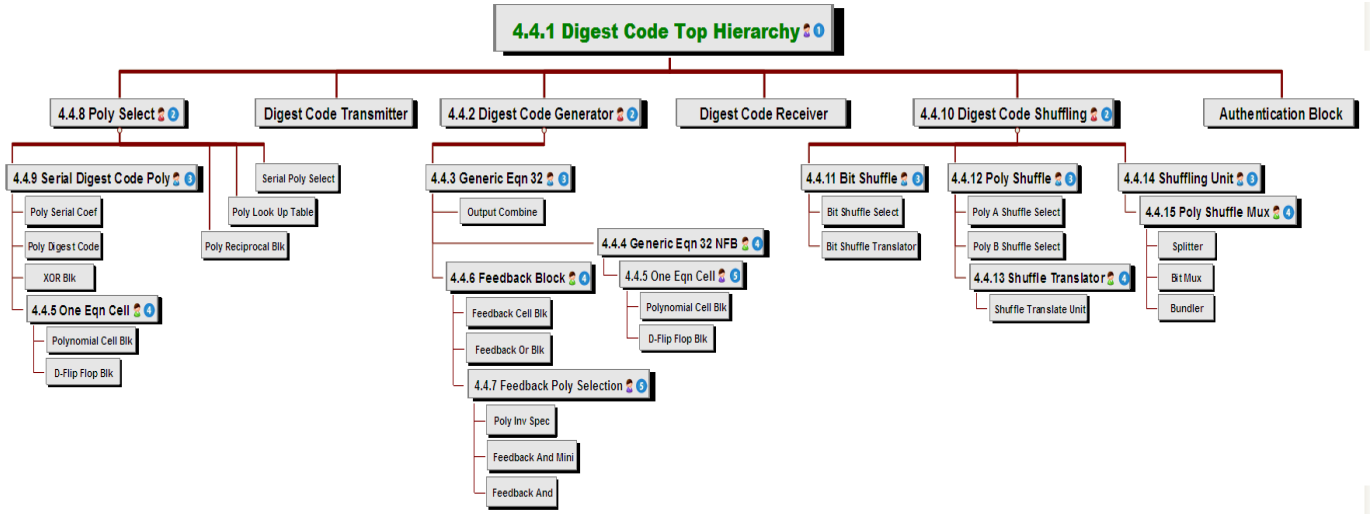

Figure 2. Design Heirarchy

C. *Digest Code Top Heirarchy Block Diagram*

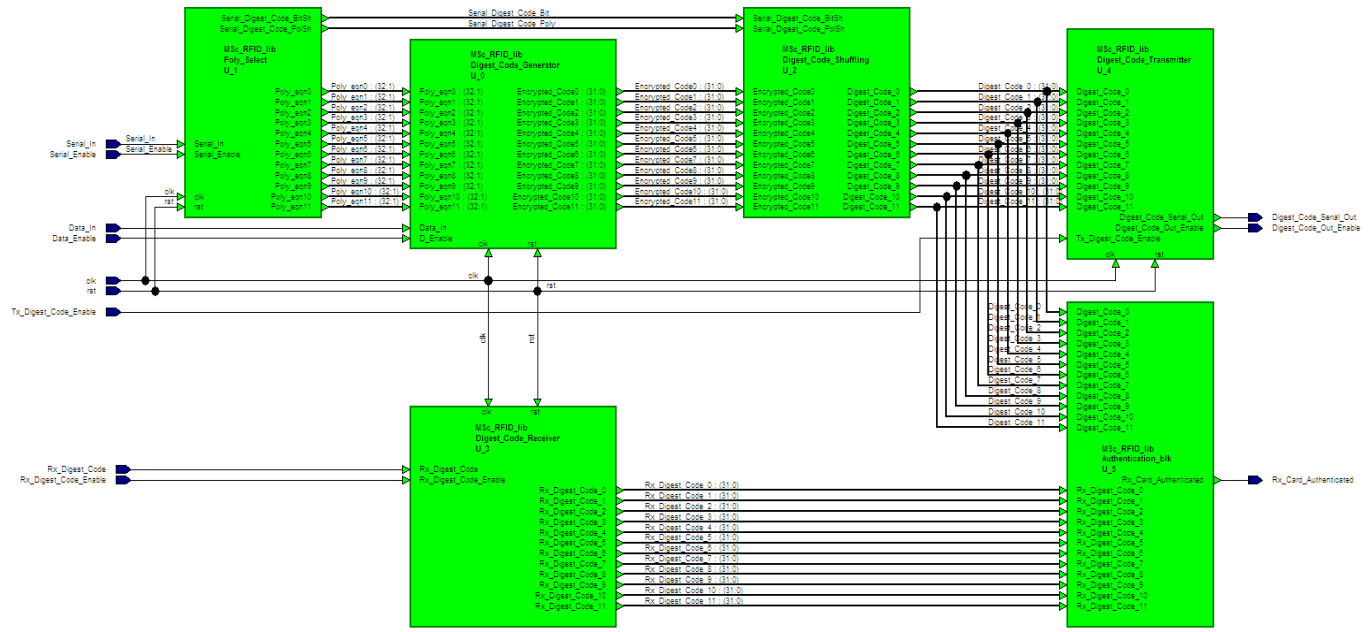

Figure 3. Digest Code Top Hierarchy Block Diagram

D. *Digest Code Top Hierarchy Describtion*

The Digest code top hierarchy consists of 6 main blocks:

1- *Poly Select.*

This block is a hierarchal block. It is responsible for selecting the polynomials used to generate the authentication code (Digest Code). It selects twelve polynomials in a random way from a pool that contains thirty two polynomials of different degrees.

2- *Digest Code Generator.*

This block is a hierarchal block. It is responsible for generating a pre-digest code using the twelve polynomials selected by the "poly select" block. This "Digest Code generator" block is built from a twelve generic hardware polynomial that work in parallel independent on each other. These twelve hardware polynomials are designed to work with any polynomial selected from the polynomial pool that contains thirty two polynomials.

3- Digest Code Shuffling.

This block is a hierarchal block. It is responsible for shuffle the pre-digest code that is generated by the "Digest Code Generator" that is automatically programmed through the selected polynomials that is selected by the "Poly Select" block. This block shuffle the pre-digest code generated by one polynomial and another as well this block is responsible for shuffling the bits from pre-digest code to another in a random way to maximize the property of being one way function.

4- Digest Code Transmitter.

This block is responsible for converting the parallel digest code 12x32bit into serial to be written on the card.

5- Digest Code Receiver.

This block is responsible for receiving serial digest code and converts it into parallel for comparison with the generated digest code.

6- Authentication Block.

This block is responsible for comparing the received digest code with the generated digest code and takes a decision whether the card is authenticated or refused due a mismatch between the card digest code and the generated digest code.

V. Design Synthesis

Xilinx ISE Version 9.2i is used for synthesis. The design and the test bench is designed using a portable VHDL code and can be mapped for any family of FPGA for any vendor like Xilinx or Altera or others and for any family like vertex, Spartan or others.

We first synthesis the design without the test bench to evaluate the usage of FPGA chip resources from Flip Flops, Look Up Tables (LUT). A detailed report found in Table II that is extracted from the synthesis tools Xilinx ISE Ver. 9.2i.

The system is implemented on FPGA Xilinx Spartan 3E using XC3E500E -5FG320 Chip.

A. Synthesis Results for the design

1- Frequency (Speed) of the design.

- Maximum Frequency (Max. Operating Frequency) is 76.530MHz.
- Minimum period is 13.067ns.

2- Timing.

- Setup time (Minimum input arrival time before clock) is 5.211ns.
- Hold Time (Maximum output required time after clock) is 4.851ns.
- Propagation Delay (Maximum combinational path delay) is 4.877ns.

One of the RFID standards in the frequency range is 13.56MHz. The International Standard Protocols for the RFID systems are ISO/IEC 14443, ISO/IEC 15693 or ISO/IEC 18000-3 have high bitrates starting from 106 Kbit/s up to 848 Kbit/s [5].

TABLE II. Synthesis Report Extracted from Xilinx tools ISE 9.2i. for our system implementation

DIGEST_CODE_TEST_BENCH_V4 Project Status			
Project File:	Digest_Code_Test_Bench_V4.ise	**Current State:**	Programming File Generated
Module Name:	Digest_Code_Test_Bench_Top_Hierarchy	**• Errors:**	No Errors
Target Device:	xc3s500e-5fg320	**• Warnings:**	792 Warnings
Product Version:	ISE 9.2i	**• Updated:**	Mon Dec 5 05:46:19 2011

DIGEST_CODE_TEST_BENCH_V4 Partition Summary
No partition information was found.

Current Errors
No Errors Found

Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of Slice Flip Flops	1,272	9,312	13%	
Number of 4 input LUTs	7,537	9,312	80%	
Logic Distribution				
Number of occupied Slices	4,269	4,656	91%	
Number of Slices containing only related logic	4,269	4,269	100%	
Number of Slices containing unrelated logic	0	4,269	0%	
Total Number of 4 input LUTs	7,546	9,312	81%	
Number used as logic	7,537			
Number used as a route-thru	9			
Number of bonded IOBs	26	232	11%	
IOB Flip Flops	2			
Number of GCLKs	2	24	8%	
Total equivalent gate count for design	62,695			
Additional JTAG gate count for IOBs	1,248			

Performance Summary			
Final Timing Score:	0	**Pinout Data:**	Pinout Report
Routing Results:	All Signals Completely Routed	**Clock Data:**	Clock Report
Timing Constraints:	All Constraints Met		

Failing Constraints
All Constraints Were Met

Clock Report					
Clock Net	**Resource**	**Locked**	**Fanout**	**Net Skew(ns)**	**Max Delay(ns)**
clk_IBUF	BUFGMUX_X1Y10	No	713	0.074	0.176
clk_IN_BUFGP	BUFGMUX_X1Y11	No	7	0.006	0.149

Detailed Reports					
Report Name	**Status**	**Generated**	**Errors**	**Warnings**	**Infos**
Synthesis Report	Current	Sun Dec 4 02:50:39 2011	0	792 Warnings	2 Infos
Translation Report	Current	Sun Dec 4 02:50:46 2011	0	0	2 Infos
Map Report	Current	Sun Dec 4 02:51:01 2011	0	0	3 Infos
Place and Route Report	Current	Mon Dec 5 05:42:56 2011	0	0	2 Infos
Static Timing Report	Current	Mon Dec 5 05:43:05 2011	0	0	3 Infos
Bitgen Report	Current	Mon Dec 5 05:46:18 2011	0	0	0

VI. System Symulation & Testing

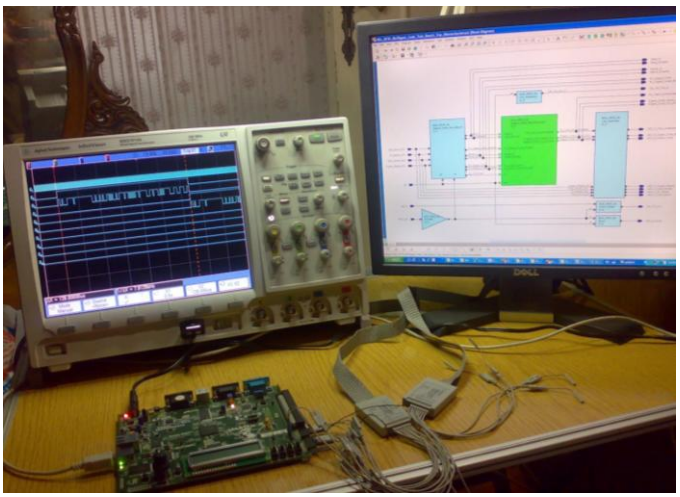

Figure 4. Hardware Test Bench Setting

Figure 5 shows the hardware testing with three packets shown on the figure, the first one is the Card ID Packet, the second one is the Data Packet and the Third one is the Digest code Packet.

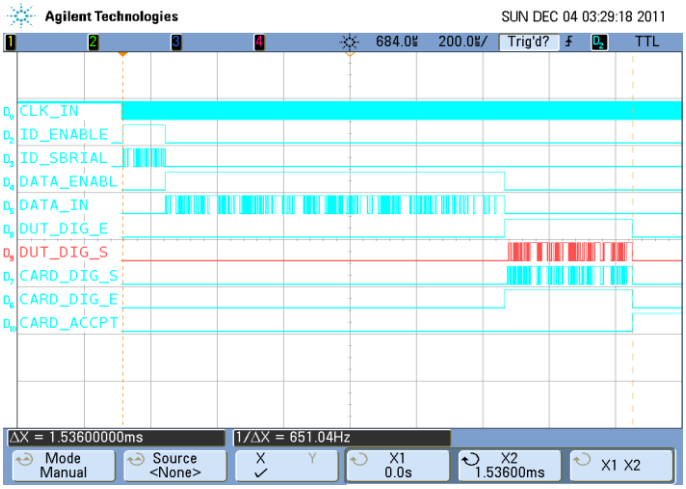

Figure 5. Hardware test with 1Kbit data packet.

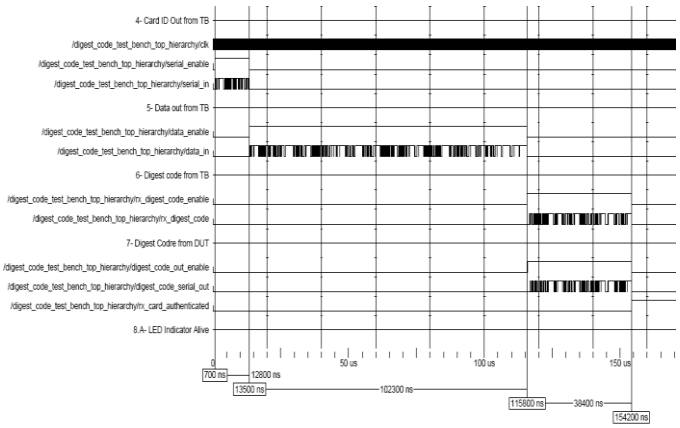

Figure 6. ModelSim Simulation for 1 Kbit data Packet.

Comparing the two figures 5 & 6, it was found that the signals are the same with the only difference is the propagation delay that differs from clock signal to output signal with maximum value of 4.877 ns.

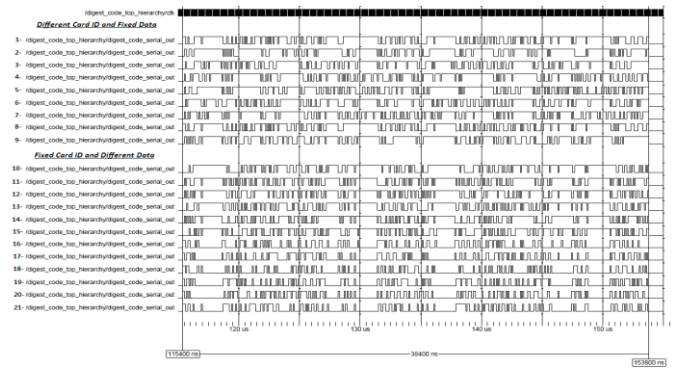

Figure 7. Authentication Code Output Comparison

Figure 7 is the consolidation of twenty one individual simulations for the whole design. It is clear that these simulations run individually since that every one of them is a test scenario by its own.

The authentication code (digest code) output is point of interest of this design; it is extracted from the simulation to be compared with each other.

This authentication code is 384 bit length. It is generated from twelve polynomial each generates thirty two bit output. These polynomials are primitive polynomials. So its period is equal to (2^r-1), where r is equal to 32 in our case, so the period is equal to (2^{32}-1) equal 4,294,967,295 bit which is much greater than 4Kbit (maximum data packet length). The twelve polynomials contain at least one of the 32 degree polynomials. So we can conclude that there is no repetition during one authentication code generation.

The change of authentication code due to the change of one bit in the data packet is large enough that it is hard to be traced, because the digest code variation due to one bit is approximately the same as if it is due to multiple bit change in the data packet.

The change of the authentication algorithm for the change of the card ID gives the design its privacy against hacking, since the hackers will work on certain card ID not all the card IDs.

The random selection for the polynomial shuffling and the bit shuffling after the polynomial selection let the tracing process tend to be impossible, which gives the design its own privacy against hacking as well.

The authentication code length 384 bit gives the combination of 3.94 x 10^{115} for every single card ID. This decreases the possibility of authentication code repetition for the same card. Every card has its own ID that gives different algorithm with totally different distribution for the authentication code with respect to the data packet on card. This means if we have two cards with same data, we will have different authentication code due to the variation of the algorithms that creates the authentication code.

VII. System Advantages and Disadvantages

The advantage of the authentication code system:

1. Speed is high enough for the present and near future applications.
2. New algorithm has been implemented for authentication with high level of protection against RFID card data interrogations.
3. Different authentication algorithm is implemented for every card ID that gives high protection level against card cloning.
4. The ability to work with multitask cards.
5. Acceptance of variable card ID length even for futuristic application and RFID EPC.
6. Easy to reconfigure the polynomials and the random LUT for every application if needed.

7. First stand alone RFID authentication process without the need of PC and backbone server for authentication.
8. The new authentication system can work with the standard RFID without the need of any modification; only append the new system to the present system.
9. Need no card processing, so it works with the standard RFID and smart card without any modifications.
10. There is no design limitation with respect to Card ID length, and data packet length.

The disadvantage of the authentication code system:

1. Adding extra bits for authentication that use part of the memory card embedded on the RFID cards.
2. More extra calculations at the reader/writer side than before.

VIII. Conclusion

One of the important issues that give a push on the technology road of the RFID technology is the cryptography science.

Cryptography science includes encryption and authentication.

Using Authentication for RFID systems in standalone devices is our research point. Our algorithm can be used as well with non-standalone system that is connected to server for database accessibility.

RFID cryptography survey is done at the beginning of the research. Finally, the review reveals that offline authentication remains unsolved as practically all existing techniques need online servers and further research is still needed in the field of offline authentication and many network issues, before RFID product authentication will meet all its promises in practice [6].

In our research we have done a Design and Implementation for the first RFID Digest Code for data authentication that prevent card cloning and card data interrogation that increase RFID card security against hacking.

New authentication algorithm is implemented with 384 bit length digest code for variable data packet length and programmable algorithm depending on variable card ID length.

Top hierarchy architecture and top down design took place through Mentor Graphic Tools FPGA Advantage Pro 7.0 tool. We used ModelSim SE Version 6.0 for simulation and Xilinx ISE Version 9.2i for synthesis. The design is implemented using a portable VHDL language and deployed on a Xilinx Spartan-3E Family on FPGA XC3S500E -5FG320.

The design parameters extracted from synthesis reported that the maximum operating frequency for the design is 76.530MHz with minimum period of 13.067ns, maximum propagation delay is 4.877ns, minimum setup time is 5.211ns, and the maximum holdup time is 4.851ns.

Test bench has been designed to synthesis RFID card operation with various IDs and data packets with successful and failure test scenarios.

The design is downloaded on Spartan-3E Kit manufactured by Digilent, and tested using Agilent MSO7014 Oscilloscope and impeded digital logic analyzer. The system works perfectly as simulated and within the operating ranges specified by the synthesis report.

The authentication system is secured against tracing and hacking by using self reconfigurable algorithm for different card IDs, random selection for twelve different polynomials from a pool of primitive polynomials and random selection of polynomial shuffling and bit shuffling for the digest code generated before getting out of our chip to the RFID card.

The design architecture is done in a way to give us the facility of changing the pool polynomials and the random functions easily if needed for different application.

This design enable RFID card multitasking as it can be used with smart card as well.

Acknowledgment

I would like to thank ALFA Electronics specially Eng. Adel Adib (CEO) for the resources of testing devices and kits and for encouraging us, and for his positive thinking towards the society.

References

[1] Jari-Pascal Curty, Michel Declercq, Catherine Dehoilain, Norbert Joehl; Ecole Polytechnique Federale de Lausanne, Switzerland; “Design and Optimization of Passive UHF RFID Systems”, 2007.

[2] Judith Symonds, John Ayoade, David Parry, “Auto-Identi. cation and Ubiquitous Computing Applications: RFID and Smart Technologies for Information Convergence”, 2009.

[3] Robert A. Kleist, Theodre A. Chapman, David A. Sakai, Brad S. Jarvis; “RFID Labelling, Smart labelling concepts & applications, for the consumer packaged goods supply chain”, 2004.

[4] Nirmal R. Saxena and Edward J. McCluskey, “Primitive Polynomial Generation Algorithms Implementation and Performance Analysis”, Technical Report, Center for Reliable Computing Stanford University, California, April 2004.

[5] Klaus Finkenzeller, “RFID Handbook, Fundamentals and application in contactless smart cards, radio frequency identification and near-field communication, third edition”, 2010.

[6] Mikko Lehtonen1, Thorsten Staake2, Florian Michahelles1, and Elgar Fleisch1,2 1Information Management, ETH Zurich, 8092 Zurich, Switzerland, 2Institute of Technology Management, University of St.Gallen, 9000 St.Gallen, Switzerland, “From Identification to Authentication – A Review of RFID Product Authentication Techniques”.